

Computing Gröbner bases for quasi-homogeneous systems

Jean-Charles Faugère*
Jean-Charles.Faugere@inria.fr

Mohab Safey El Din*
Mohab.Safey@lip6.fr

Thibaut Verron†*
Thibaut.Verron@ens.fr

*INRIA, Paris-Rocquencourt Center, PolSys Project
UPMC, Univ. Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy-Kennedy
Case 169, 4, Place Jussieu, F-75252 Paris

†École Normale Supérieure,
45, rue d'Ulm, F-75230, Paris

ABSTRACT

Let K be a field and $(f_1, \dots, f_n) \subset \mathbb{K}[X_1, \dots, X_n]$ be a sequence of quasi-homogeneous polynomials of respective weighted degrees (d_1, \dots, d_n) . By this, we mean that there exists $(w_1, \dots, w_n) \in \mathbb{Z}_{>0}^n$ s.t. for any $1 \leq j \leq n$, the polynomial $f_i(X_1^{w_1}, \dots, X_n^{w_n})$ is homogeneous and has degree d_i . This paper focuses on designing strategies for computing Gröbner bases of such systems.

Under some genericity assumptions on the coefficients of the f_i 's, we prove the bound $(\sum_{i=1}^n (d_i - w_i)) + \max\{w_i\}$ on the degree of regularity of such systems. This is done by using well-known results on Hilbert series and designing a dedicated quasi-homogeneous matrix- F_5 algorithm taking care of this structure. We provide a detailed complexity analysis of this algorithm, and we prove that we can divide the complexity bounds by P^ω , where $P = \prod_{i=1}^n w_i$. We also show how to use the FGLM (change of ordering) step in this special setting to obtain a Gröbner basis for the lexicographical ordering in time polynomial in the weighted Bézout bound $\prod_{i=1}^n \frac{d_i}{w_i}$.

All in all, we provide a complete computational strategy for solving quasi-homogeneous systems in time polynomial in this weighted Bézout bound. We finally prove that these complexity results apply for 0-dimensional affine systems which are obtained by specializing to 1 a variable in a quasi-homogeneous system. We provide some experiments showing that this computational strategy sometimes offer gains of up to 10, and allows to handle systems which cannot be tackled with previous approaches.

1. INTRODUCTION

Motivation and problem statement. Polynomial systems solving is a very important problem in computer algebra, with a wide range of applications in theory (algorithmic geometry) or in real life (cryptography). For this purpose, Gröbner bases of polynomial ideals are a valuable tool, and

practicable computation of the Gröbner bases of any given ideal is a major challenge of modern computer algebra. Since their introduction in 1965, many algorithms have been designed to compute Gröbner bases ([6, 9, 10, 13]), allowing for more and more systems to be solved.

Systems arising from “real life” problems often show some structure easing the Gröbner basis computation. For example, it is known that homogeneous systems, or system with an important maximal homogeneous component, are better solved by using a degree-compatible order, and then applying a change of ordering. In this paper, we study a structure slightly more general than homogeneity, called *quasi-homogeneity*. More precisely, we will say that a polynomial $P(X_1, \dots, X_n)$ is quasi-homogeneous for the *system of weights* $W = (w_1, \dots, w_n)$, if the polynomial

$$Q(Y_1, \dots, Y_n) := P(Y_1^{w_1}, \dots, Y_n^{w_n})$$

is homogeneous. Systems with such a structure are likely to arise for example from physics, where all measures are associated with a dimension which, to some extent, we can see as a weight.

Let $F = (f_1, \dots, f_m)$ be a zero-dimensional system of quasi-homogeneous polynomials (or of polynomials with an important maximal quasi-homogeneous component), it is possible to try to compute directly a Gröbner basis of the ideal generated by F , ignoring the quasi-homogeneous structure. However, there is no general way of evaluating the complexity of this strategy.

Another approach is to compute the *homogenized* system $\tilde{F} := (f_i(X_1^{w_1}, \dots, X_n^{w_n}))$ and then compute a Gröbner basis of that system, using the usual strategies for the homogeneous structure. The first step of the computation proves much faster than with the naive strategy, but the change of ordering is slowed down, and thus becomes the main bottleneck of the computation. This leads to the following three questions :

1. Is this strategy valid: does a Gröbner basis of the ideal generated by \tilde{F} give any information regarding a Gröbner basis of $\langle F \rangle$?
2. Can we obtain a similar speedup for the change of ordering?
3. Can we evaluate the complexity of this strategy, and thus explain these speedups?

Main results. For the strategy consisting in ignoring the quasi-homogeneous structure of the system, there is no precise complexity estimate. On the other hand, in this paper,

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 20XX ACM X-XXXXX-XX-X/XX/XX ...\$10.00.

we offer a full strategy to compute a lexicographical Gröbner basis of a quasi-homogeneous zero-dimensional system, with complexity results under genericity assumptions, so that the answer to the three questions above is positive.

More precisely, we define in a natural way a weighted variant of the GREVLEX ordering, which we call the W -GREVLEX ordering. We then prove that a GREVLEX Gröbner basis of $\langle \tilde{F} \rangle$ provides a W -GREVLEX Gröbner basis of $\langle F \rangle$, and we can use the FGLM algorithm to perform the change of ordering to the LEX ordering, without any slowdown. For complexity results, we will assume the system to satisfy the two following generic conditions:

- H1.** The sequence f_1, \dots, f_m is regular;
- H2.** The sequence f_1, \dots, f_i is in Noether position w.r.t. X_1, \dots, X_i , for any $1 \leq i \leq m$.

Under the hypothesis **H1**, we adapt the known results of the homogeneous case, using similar arguments based on Hilbert series, to give estimates on the degree of the ideal and the degree of regularity of the system :

$$\deg(I) = \prod_{i=1}^n \frac{d_i}{w_i}; \quad d_{\text{reg}}(F) \leq \sum_{i=1}^n (d_i - w_i) + \max\{w_i\}.$$

We also present a variant of the matrix- F_5 algorithm which follows more closely the behavior of F_5 ran on \tilde{F} . A combinatorial result found in [1] shows that the number of columns of the matrices appearing in that variant of matrix- F_5 is approximately divided by $\prod_{i=1}^n w_i$, when compared to the regular matrix- F_5 algorithm. In the end, we show that for systems satisfying **H1**, our strategy, using our variant of matrix- F_5 and FGLM, performs in time polynomial in $\prod_{i=1}^n d_i / \prod_{i=1}^n w_i$, that is polynomial in the number of solutions.

Further assuming the hypothesis **H2**, we also carry on the precise complexity analyses done in [2] for homogeneous systems, and adapt them to the quasi-homogeneous case to deduce a precise complexity bound for our quasi-homogeneous variant of Matrix- F_5 . It confirms that overall, we are able to compute a LEX Gröbner basis for a generic quasi-homogeneous system P^ω times faster than for a generic homogeneous system, where $P = \prod_{i=1}^n w_i$.

We have been able to run benchmarks on both generic systems and real-life systems arising in cryptography. Experimentally, in both cases, our strategy seems always faster than ignoring the quasi-homogeneous structure, the gain increasing with the considered weights.

Experiments have also shown that the order of the variables can have an impact on the performances of both strategies, predicting it seems to require more sophisticated tools and is left to further work.

Prior works. Making use of the structure of polynomial systems to develop faster algorithms has been a general trend over the past few years: see for example [14], [7] or [15]. Polynomial algebras graded with respect to a system of weights have been studied from the sight of commutative algebra. Most notably, the Hilbert series of ideals defined by regular sequences, which we use several times in this paper, is well known, and could be found for example in [19]. The paper [18] defines many structures of polynomial algebras, including weighted gradings, in preparation for future algorithmic developments. Combinatorial objects arising when we try to estimate the number of monomials of a given W -degree are called *Sylvester denominants*, and studied for example in [1].

When it comes to Gröbner bases, weighted gradings and related orderings have been described in early works such as [4]. However, as far as we know, the impact of a quasi-homogeneous structure on the complexity of Gröbner bases computations had never been studied.

Amongst the various computer algebra software able to compute Gröbner bases, it seems only Magma [5] is taking advantage of a system of weights, and if available, uses the W -GREVLEX ordering to compute an intermediate basis before the change of ordering. Moreover, it is able to retrieve the appropriate system of weights. However, this strategy is only available for quasi-homogeneous systems.

Structure of the paper. In section 2 we define more precisely quasi-homogeneous systems, and we compute their degree and degree of regularity assuming the above hypotheses. We also take this occasion to quickly show that these hypotheses are generic. In section 3 we prove that the strategy consisting of modifying the system is correct, we explain how we can adapt matrix- F_5 and FGLM to quasi-homogeneous systems, and then we evaluate the complexity of these algorithms. In section 4, we briefly explain how these results for quasi-homogeneous systems still help in case the system is obtained from a quasi-homogeneous system, by specializing one of the variables to 1. We also give an example of such a structure, as well as the associated algorithm. Finally, in section 5, we give some experimental results.

2. QUASI-HOMOGENEOUS SYSTEMS

2.1 Weighted degrees and polynomials

Let \mathbb{K} be a field, we consider the algebra $A := \mathbb{K}[X_1, \dots, X_n] = \mathbb{K}[\mathbf{X}]$. Even though usually, one uses the total degree to grade the algebra A , there are other ways to define such a grading, as seen in [4], for example.

Definition 1. Let $W = (w_1, \dots, w_n)$ be a vector of positive integers. Let $\alpha = (\alpha_1, \dots, \alpha_n)$ be a n -uple of nonnegative integers, we call W -degree, or *weighted degree* of a monomial $\mathbf{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ the integer $\deg_W(\mathbf{X}^\alpha) = \sum_{i=1}^n w_i \alpha_i$. The vector W is called *system of weights*. We denote by $\mathbf{1}$ the weight system defined by $(1, \dots, 1)$, associated with the usual grading on A .

One can prove that any grading on $\mathbb{K}[\mathbf{X}]$ comes from such a weight system ([4, sec. 10.2]). We denote by $(\mathbb{K}[\mathbf{X}], W)$ the W -graded structure on A , and in that case, to avoid ambiguities, we use the adjective *W-homogeneous* for elements or ideals, or *quasi-homogeneous* if W is clear in the context. The word *homogeneous* will be reserved to $\mathbf{1}$ -homogeneous items.

PROPOSITION 1. Let $(\mathbb{K}[X_1, \dots, X_n], W)$ be a graded polynomial algebra. Then the application

$$\begin{aligned} \text{hom}_W : (\mathbb{K}[X_1, \dots, X_n], W) &\rightarrow (\mathbb{K}[t_1, \dots, t_n], \mathbf{1}) \\ f &\mapsto f(t_1^{w_1}, \dots, t_n^{w_n}) \end{aligned}$$

is an injective graded morphism, and in particular the image of a quasi-homogeneous polynomial is a homogeneous polynomial.

PROOF. It is an easy consequence of the definition of the weighted grading. \square

The above morphism also provides a quasi-homogeneous variant of the GREVLEX ordering, which we call the W -GREVLEX ordering:

$$u <_{W\text{-grevlex}} v \iff \text{hom}_W(v) <_{\text{grevlex}} \text{hom}_W(v)$$

Given a W -homogeneous system F , one can build the homogeneous system $\text{hom}_W(F)$, and then apply classical algorithms ([10, 13]) to that system to compute a GREVLEX (resp. LEX) Gröbner basis of the ideal generated by $\text{hom}_W(F)$. We will prove in section 3 (prop. 7) that this basis is contained in the image of hom_W , and that its pullback is a W -GREVLEX (resp. LEX) Gröbner basis of the ideal generated by F .

Let us end this paragraph with some notations and definitions. We call *degree of regularity* of the system F the highest degree $d_{\text{reg}}(F)$ reached in a run of F_5 to compute a GREVLEX Gröbner basis of $\text{hom}_W(F)$. We call *index of regularity* of an ideal I the degree i_{reg} of the Hilbert series $\text{HS}_{A/I}$, defined as the difference of the degree of its numerator and the degree of its denominator.

Recall that given a homogeneous ideal I , we define its degree D as the degree of the projective variety $V(I)$, as introduced for example in [16]. This definition still holds for the quasi-homogeneous case. In case the projective variety is empty, that is if the affine variety is equal to $\{0\}$, we extend that definition by letting D be the multiplicity of the 0 point, that is the dimension of the \mathbb{K} -vector space A/I . Finally, from now on we will only consider *affine* varieties, even when the ideal will be quasi-homogeneous. It means in particular that the dimension of $V(0)$ is n , and that a zero-dimensional variety will be defined by at least n polynomials.

2.2 Degree and degree of regularity

Zero-dimensional regular sequences. As in the homogeneous case, regular sequences are an important case to study, because it is a generic property which allows us to compute several key parameters and good complexity bounds. We first show how we can compute the degree, and a bound on the degree of regularity of a zero-dimensional ideal defined by a regular sequence.

THEOREM 2. *Let $W = (w_1, \dots, w_n)$ be a weight system, and $F = (f_1, \dots, f_m)$ a regular sequence of W -homogeneous polynomials, of respective W -degrees d_1, \dots, d_m . Further assume that the set of solutions is zero-dimensional, that is $m = n$. We denote by I the quasi-homogeneous ideal generated by F . Then we have $\deg(I) = \prod_{i=1}^n \frac{d_i}{w_i}$ and $d_{\text{reg}}(F) \leq \sum_{i=1}^n (d_i - w_i)$.*

PROOF. We will read the degree and degree of regularity of the system on the Hilbert series (or Poincaré series) of the algebra A/I . A classical result which can be found for example in [19, cor. 3.3] states that, for regular sequences, this series is

$$\text{HS}_{A/I}(t) = \frac{(1 - t^{d_1}) \cdots (1 - t^{d_m})}{(1 - t^{w_1}) \cdots (1 - t^{w_n})}. \quad (1)$$

We assumed $n = m$, so the Hilbert series can be rewritten as

$$\text{HS}_{A/I}(t) = \frac{(1 + \cdots + t^{d_1-1}) \cdots (1 + \cdots + t^{d_n-1})}{(1 + \cdots + t^{w_1-1}) \cdots (1 + \cdots + t^{w_n-1})}.$$

In the 0-dimensional case, recall that the Hilbert series is actually a polynomial, and has degree $i_{\text{reg}} = \sum_{i=1}^n (d_i - w_i)$. This means that all monomials of W -degree greater than i_{reg} are in the ideal, and as such, that the leading terms of the W -GREVLEX Gröbner basis of F need to divide all the monomials of W -degree greater than i_{reg} . This proves that all the polynomials in the Gröbner basis computed by F_5 have W -degree at most $i_{\text{reg}} + \max\{w_i\}$. And since the F_5 criterion ([10]) ensures that there is no degree-fall in a run of F_5 on a regular sequence, the algorithm indeed stops in degree at most $i_{\text{reg}} + \max\{w_i\}$.

Furthermore, the degree of the ideal I is equal to the dimension of the vector space A/I , that is the value of the Hilbert series at $t = 1$, that is $\prod_{i=1}^n \frac{d_i}{w_i}$. \square

Note that except for this inequality, not much is known about the degree of regularity of a quasi-homogeneous system. In particular, the above bound is nothing more than a bound, even in the generic case. Let me introduce some examples of the three cases one can observe with a quasi-homogeneous generic system:

1. $W = (3, 2, 1)$, generic system of W -degree $\mathbf{D} = (6, 6, 6)$: then $d_{\text{reg}} = i_{\text{reg}} + 1 = 13$;
2. $W = (1, 2, 3)$, generic system of W -degree $\mathbf{D} = (6, 6, 6)$: then $d_{\text{reg}} = 15 > i_{\text{reg}} + 1 = 13$;
3. $W = (2, 3)$, generic system of W -degree $\mathbf{D} = (6, 6)$: then $d_{\text{reg}} = 6 < i_{\text{reg}} = 7$.

Only the case 1 is observed with generic homogeneous systems. Furthermore, examples 1 and 2 show that the degree of regularity depends on the order of the variables (chosen in the description of the weight system). As the Hilbert series of a generic sequence doesn't depend on that order, it shows that we probably need to find a better tool in order to evaluate more precisely the degree of regularity in the quasi-homogeneous case. However, the above bound already leads to good improvements on the complexity bounds, as we will see in the following sections. Also note that these computations only hold when the system is 0-dimensional, we will discuss that restriction in section 2.3.

Genericity. We now prove that zero-dimensional W -homogeneous sequences of given W -degree are generically regular, under some assumptions on the W -degree. Let's start with the first part of this statement:

LEMMA 3. *Let n be a positive integer, and consider the algebra $A := \mathbb{K}[X_1, \dots, X_n]$, graded with respect to the system of weights $W = (w_1, \dots, w_n)$. Regular sequences of length n form a Zariski-open subset of all sequences of quasi-homogeneous polynomials of given W -degree in A .*

PROOF. Let (d_1, \dots, d_m) be a family of W -degrees, we consider the set $V(\mathbb{K}[\mathbf{a}][\mathbf{X}])$ of all systems of quasi-homogeneous polynomials of W -degree d_1, \dots, d_m . We denote by f_1, \dots, f_m the polynomials of the generic system, and by I the ideal they generate, in $\mathbb{K}[\mathbf{a}][\mathbf{X}]$.

Since the Hilbert series (1) characterizes regular sequences ([19, cor. 3.2]), the sequence (f_i) is regular if and only if the ideal I contains all monomials of W -degree between $i_{\text{reg}}(I) + 1$ and $i_{\text{reg}}(I) + \max\{w_i\}$, where $i_{\text{reg}}(I)$ is given by $\sum(d_i - w_i)$. This expresses that a given set of linear equations have solutions, and so it can be coded as some determinants being non-zero. \square

There are some systems of W -degree for which there is no regular sequence. The reason is that because of the weights, for some systems of W -degrees, there exists no or very few monomials. For example, take $n = 2$, $W = (1, 2)$ and $\mathbf{D} = (1, 1)$. All quasi-homogeneous polynomials of W -degree 1 are in $\mathbb{K}X$, so there is no regular sequence of quasi-homogeneous polynomials with these W -degrees.

However, if we only consider "reasonable" systems of W -degrees, that is systems of W -degrees for which there exists a regular sequence, regular sequences form a Zariski-dense subset from the above.

Remark 1. A sufficient condition for example is to take W -degrees such that w_1 is divisible by d_1, \dots, w_n is divisible by

d_n . This way we can define the sequence $X_1^{d_1/w_1}, \dots, X_n^{d_n/w_n}$, which is regular, and so for such systems of weight, the regularity condition is generic.

We only proved the genericity for quasi-homogeneous sequences of length n , the more general case of a sequence of length $m \leq n$ will be proved in section 2.3 (remark 2).

2.3 Noether position

To compute the degree and degree of regularity of quasi-homogeneous systems of positive dimension, we will assume that the system $F = \langle f_1, \dots, f_m \rangle$ we consider is in *Noether position* (as seen in [8, ch. 13, sec. 1] or [3, def. 2]), i.e.

- for $i \leq m$, the canonical image of X_i in $\mathbb{K}[\mathbf{X}]/I$ is an algebraic integer over $\mathbb{K}[X_{m+1}, \dots, X_n]$;
- $\mathbb{K}[X_{m+1}, \dots, X_n] \cap I = 0$.

LEMMA 4. *Let $F = f_1, \dots, f_m$ be a regular quasi-homogeneous sequence of polynomials in $\mathbb{K}[X_1, \dots, X_n]$. The sequence F is in Noether position if and only if the sequence $F_{\text{ext}} := f_1, \dots, f_m, X_{m+1}, \dots, X_n$ is regular.*

PROOF. Let I be the ideal generated by the f_i 's. The geometric characterization of Noether position (see e.g. [17]) shows that the canonical projection onto the m first coordinates $\pi : V(I) \rightarrow V(\langle X_1, \dots, X_m \rangle)$ is a surjective morphism with finite fibers. This implies that the variety $V(\langle F_{\text{ext}} \rangle)$, that is $\pi^{-1}(0)$, is zero-dimensional, and so the sequence is regular.

Conversely, assume F_{ext} is a regular sequence. We want to show that every X_i for $i \leq m$ is integral over the ring $\mathbb{K}[X_{m+1}, \dots, X_n]$. Since it defines a zero-dimensional ideal, for any i , there exists $n_i \in \mathbb{N}$ such that $X_i^{n_i} = \text{LT}(f)$ with $f \in \langle F_{\text{ext}} \rangle$ for the GREVLEX ordering with $X_1 > \dots > X_n$. By definition of the GREVLEX ordering, we can assume that f simply belongs to I . This shows that every X_i is integral over $\mathbb{K}[X_{m+1}, \dots, X_n]/I$. We get the requested result by induction on i : first, this is clear if $i = m$. Now assume that we know that $\mathbb{K}[X_i, \dots, X_n]/I$ is an integral extension of $\mathbb{K}[X_{m+1}, \dots, X_n]$. From the above, we also know that X_{i-1} is integral over $\mathbb{K}[X_i, \dots, X_n]$, and so, since the composition of integral homomorphisms is integral, we get the requested result.

Finally, we want to check the second part of the definition of Noether position. Assume that there is a non-zero polynomial in $\mathbb{K}[X_{m+1}, \dots, X_n] \cap I$, since the ideal is quasi-homogeneous, we can assume this polynomial to be quasi-homogeneous. Either this polynomial is of degree 0, either it is a non-trivial syzygy between X_{m+1}, \dots, X_n , so either way, it contradicts the regularity hypothesis. \square

As we did for regular sequences, we first show how we can evaluate the degree and degree of regularity of a sequence in Noether position, and then we show that the Noether position property is generic under some assumptions on the W -degree of the polynomials.

THEOREM 5. *Let $W = (w_1, \dots, w_n)$ be a weight system, and f_1, \dots, f_m a regular sequence in Noether position, of quasi-homogeneous polynomials of W -degrees (d_1, \dots, d_m) . The same way we did above, we denote by I the ideal generated by the f_i 's. Then we have $\deg(I) = \prod_{i=1}^m \frac{d_i}{w_i}$ and $d_{\text{reg}}(I) \leq \sum_{i=1}^m (d_i - w_i) + \max\{w_i\}$.*

PROOF. Let us denote by I' the ideal generated by F_{ext} . The degree of the ideal I' is the same as that of I , because the variety it defines is the intersection of $V(I)$ with some

non-zero-divisor hyperplanes. Furthermore, all critical pairs appearing in a run of F_5 on F will also appear in a run of F_5 on F_{ext} , ensuring that $d_{\text{reg}}(F) \leq d_{\text{reg}}(F_{\text{ext}})$.

But since by Noether position, the family F_{ext} defines a zero-dimensional variety, we can use the previous computations to deduce its degree of regularity and the degree of I' . \square

LEMMA 6. *Let n be a positive integer, and consider the algebra $A := \mathbb{K}[X_1, \dots, X_n]$, graded with respect to the system of weights $W = (w_1, \dots, w_n)$. Systems in Noether position form a Zariski-open subset of all systems of quasi-homogeneous polynomials of given W -degrees in A .*

PROOF. Let $F = (f_1, \dots, f_m)$ be m generic quasi-homogeneous polynomials, with coefficients in $\mathbb{K}[\mathbf{a}]$. We use the same characterization of a zero-dimensional regular sequence as we did in the proof of Lemma 3. It allows us to express the regularity condition for the sequence $(f_1, \dots, f_m, X_{m+1}, \dots, X_n)$ as some determinants being non-zero, which by definition, shows that the condition of being in Noether position is an open condition. \square

Since a sequence in Noether position is in particular a regular sequence, we are confronted with the same problem as for the genericity of regular sequences, that is the possible emptiness of the condition. However, it is still true that for “reasonable” systems of W -degrees, that is systems of W -degrees for which there exists enough monomials, sequences in Noether position do exist, and thus form a Zariski-dense subset of all sequences. For example, since the sequence $X_1^{d_1/w_1}, \dots, X_m^{d_m/w_m}$ is in Noether position, the sufficient condition given in Remark 1 is also sufficient to ensure that sequences in Noether position are Zariski-dense.

Remark 2. Any sequence in Noether position is in particular a regular sequence, so Lemma 6 proves that, under the same assumption on the degree, regular sequences of length $m \leq n$ are generic amongst quasi-homogeneous sequences of given W -degree.

3. COMPUTING GRÖBNER BASES

3.1 Using the standard algorithms on the homogenized system

As we said before, in order to apply the F_5 algorithm to a quasi-homogeneous system, we may run it through hom_W . This is shown by the following proposition.

PROPOSITION 7. *Let $F = (f_1, \dots, f_m)$ be a family of polynomials in $\mathbb{K}[X_1, \dots, X_n]$, assumed to be quasi-homogeneous for a weight system $W = (w_1, \dots, w_n)$. Let $<_1$ be a monomial order, G the reduced Gröbner basis of $\text{hom}_W(F)$ for this order, and $<_2$ the pullback of $<_1$ through hom_W . Then*

1. *all elements of G are in the image of hom_W ;*
2. *the family $G' := \text{hom}_W^{-1}(G)$ is a reduced Gröbner basis of the system F for the order $<_2$.*

PROOF. For the first statement, it is enough to notice that we can compute such a reduced Gröbner basis by applying the Buchberger algorithm and reducing that base. Both steps only involve computations of S -polynomials, and one checks that $S\text{-Pol}(\text{hom}_W(f), \text{hom}_W(g)) = \text{hom}_W(S\text{-Pol}(f, g))$. So at the end of the computations, all polynomials in the basis are in the image of hom_W .

For the second assertion, let us first notice that since $<_2$ is the reverse image of $<_1$ by hom_W , one has, for any polynomial f , $\text{hom}_W^{-1}(\text{LT}(f)) = \text{LT}(\text{hom}_W^{-1}(f))$ and so G' is indeed

a Gröbner basis of $\langle G' \rangle$. What remains to check now is that this ideal is equal to $\langle F \rangle$. This makes use of the following lemma:

LEMMA 8. *Let $P = (p_1, \dots, p_k)$ be a family of polynomials, then $\text{hom}_W^{-1}(\langle \text{hom}_W(P) \rangle) = \langle P \rangle$.*

PROOF. The reverse inclusion is easy: if $f = \sum q_i p_i \in \langle P \rangle$ then $\text{hom}_W(f) = \sum \text{hom}_W(q_i) \text{hom}_W(p_i) \in \langle \text{hom}_W(P) \rangle$. Let's prove the direct inclusion. Let g be a polynomial in $\text{hom}_W^{-1}(\langle \text{hom}_W(P) \rangle)$, there exist polynomials g_i such that $\text{hom}_W(g) = \sum g_i \text{hom}_W(p_i)$.

Separating the monomials between those which are in $\text{hom}_W(\mathbb{K}[\mathbf{X}])$ and those which aren't, we have a decomposition of all g_i 's as $g_i = \text{hom}_W(q_i) + r_i$, where no monomial of r_i is in $\text{hom}_W(\mathbb{K}[\mathbf{X}])$. So we have the decomposition $\text{hom}_W(g) = \text{hom}_W(\sum q_i p_i) + \sum r_i \text{hom}_W(p_i)$.

So we want to show that the second term in that sum is zero. This is true, because if two polynomials p and q are made only of monomials out of $\text{hom}_W(\mathbb{K}[\mathbf{X}])$, their sum is either also made only of such monomials, either zero. So here we have $\sum r_i \text{hom}_W(p_i) = 0$, and so $\text{hom}_W(g) = \text{hom}_W(\sum q_i p_i)$. Since the morphism hom_W is injective, this shows that $g = \sum q_i p_i \in \langle P \rangle$. \square

Applying that lemma twice, one checks that

$$\langle G' \rangle = \text{hom}_W^{-1}(\langle \text{hom}_W(G') \rangle) = \text{hom}_W^{-1}(\langle G \rangle)$$

$$= \text{hom}_W^{-1}(\langle \text{hom}_W(F) \rangle) = \langle F \rangle,$$

which is the wanted result. \square

In practice, if we want to compute a LEX Gröbner basis of F , we generate the system $\tilde{F} = \text{hom}_W(F)$, we compute a GREVLEX basis \tilde{G}_1 of \tilde{F} with F_5 or matrix- F_5 , and then we compute a LEX Gröbner basis \tilde{G}_2 of \tilde{F} with FGLM. In the end, we get a LEX Gröbner basis of \tilde{F} , which we turn into a LEX Gröbner basis of F via hom_W^{-1} .

We immediately notice that this method has several drawbacks for both matrix- F_5 and FGLM: we have seen, at least for regular sequences, that going through hom_W increases the degree and the known bound for the degree of regularity of the system. Furthermore, for a given integer d , there are way more monomials of 1-degree d than of W -degree d . This results in matrix- F_5 working with matrices that are larger than necessary.

3.2 Direct algorithms

Let us first consider the problem of the change of ordering. In the above process, we can apply hom_W^{-1} to the basis \tilde{G}_1 and this way obtain a W -GREVLEX basis G_1 of F . We can then run FGLM on that basis to obtain a LEX basis of F . This way, we can avoid the problem of a greater degree of the ideal on the complexity of the FGLM step.

About matrix- F_5 , we can also avoid going through hom_W , all we have to do is to change the algorithm a little, in order to directly consider the variables with their weight. The modified algorithm is algorithm 1 opposite. The function $\text{F5CRITERION}(\mu, i, \mathcal{M})$ implements the F_5 -criterion described in [10]: it evaluates to false if and only if μ is the leading term of a line of the matrix $\mathcal{M}_{d-d_i, i-1}$. The function $\text{ECHELONFORM}(M)$ reduces the matrix M to row-echelon form, not allowing any row swap.

The only part that differs from the classical matrix- F_5 is the loop, from line 9 to line 15. Recall that the classical algorithm loops on the labels (e, f_i) in degree $d-1$, and check the F_5 criterion on all new monomials of degree $(d - \deg(f_i))$ one can obtain from e . Instead, this algorithm loops on

Algorithm 1: Matrix- F_5 (W -homogeneous version)

Input: $\begin{cases} f_1, \dots, f_m \text{ } W\text{-homogeneous polynomials} \\ d_{\max} \in \mathbb{N} \end{cases}$
Output: G Gröbner basis of $\langle f_1, \dots, f_m \rangle$ up to W -degree d_{\max}

```

1  $G \leftarrow \{f_1, \dots, f_m\}$ ;
2 for  $d = 1$  to  $d_{\max}$  do
3    $\mathcal{M}_{d,0} \leftarrow$  matrix with 0 lines;
4   for  $i = 1$  to  $m$  do
5     if  $d = \deg(f_i)$  then
6        $\mathcal{M}_{d,i} \leftarrow \mathcal{M}_{d,i-1} \cup$  ligne  $f_i$  with label  $(1, f_i)$ ;
7     else if  $d > \deg(f_i)$  then
8        $\mathcal{M}_{d,i} \leftarrow \mathcal{M}_{d,i-1}$ ;
9       foreach  $\mu$  monomial of  $W$ -degree  $d - \deg(f_i)$  do
10        if  $\text{F5CRITERION}(\mu, i, \mathcal{M})$  then
11           $x_j \leftarrow$  biggest variable dividing  $\mu$ ;
12           $e \leftarrow \mu/x_j$ ;
13          if there exists a line of label  $(e, f_i)$  in  $\mathcal{M}_{d-w_j, i}$  then
14             $f \leftarrow$  reduced polynomial associated to that line;
15             $\mathcal{M}_{d,i} \leftarrow \mathcal{M}_{d,i} \cup x_j f$  with label  $(\mu, f_i)$ ;
16    $\mathcal{M}_{d,m} \leftarrow \text{ECHELONFORM}(\mathcal{M}_{d,m})$ ;
17   For any line having been reduced to a non-zero polynomial, append it to  $G$ ;
18 return  $G$ 
```

monomials of W -degree $(d - \deg(f_i))$, checks the F_5 criterion on these monomials, and then only checks if there's a label (e, f_i) (possibly in W -degree lower than $d-1$) which might lead to that monomial.

Note that the F_5 algorithm with critical pairs selects the polynomials it reduces in a finer way than the matrix- F_5 algorithm. In the W -homogeneous case, applied on \tilde{F} , it will automatically "jump" from W -degree d to W -degree $d + w_i$, without considering the parasite monomials. This gives an explanation to the fact that the F_5 algorithm seems to run much faster on homogeneous systems obtained through hom_W than on generic homogeneous systems.

3.3 First complexity bounds

Let $F = (f_1, \dots, f_n)$ be a system of W -homogeneous polynomials in $\mathbb{K}[X_1, \dots, X_n]$, and let I be the ideal generated by F , D the degree of I , d_{reg} its degree of regularity and i_{reg} its index of regularity. The classical complexity bounds of matrix- F_5 (for a regular system) and FGLM are

$$C_{F_5} = O(d_{\text{reg}} M_{d_{\text{reg}}, W}(n)^\omega); C_{FGLM} = O(nD^3),$$

where $M_{d,W}(n)$ stands for the number of monomials of W -degree d in n variables.

Assuming the system F is a regular sequence, we have already seen the following estimates: $d_{\text{reg}} \leq i_{\text{reg}} + \max\{w_i\}$ and $D = \prod_{i=1}^n d_i / \prod_{i=1}^n w_i$. If we compare these values with their equivalent with the system of weights $\mathbf{1}$, we notice an important gain in complexity in the FGLM algorithm, as well as a significant practical gain in matrix- F_5 .

But the real gain in matrix- F_5 is way more important, because the matrices of polynomials of given W -degree are much smaller than the matrices of polynomials of given

1-degree. The point of the following lemma is to evaluate this difference.

LEMMA 9. Let $W = (w_1, \dots, w_n)$ be a weight system, and for any i , let $W_i = (w_1, \dots, w_i)$. For any integer d , we denote by $M_{d,W}(n)$ the number of monomials of W -degree d , that is the size of the matrix of W -degree d . Let $\delta := \gcd(W)$, $P := \prod_{i=1}^n w_i$, S_i the integer defined recursively as following:

$$S_1 = 0, S_i = S_{i-1} + w_i \cdot \frac{\gcd(W_{i-1})}{\gcd(W_i)} \text{ for } i \geq 2$$

and T_i the integer defined recursively as following:

$$T_1 = 0, T_i = T_{i-1} + w_i \cdot \left(\frac{\gcd(W_{i-1})}{\gcd(W_i)} - 1 \right) - 1 \text{ for } i \geq 2.$$

Then the number of monomials of W -degree d is bounded above and below by:

$$\frac{\delta}{P} M_{d-T_n-n+1,1}(n) \leq M_{d,W}(n) \leq \frac{\delta}{P} M_{d+S_n-n+1,1}(n).$$

PROOF. This is a consequence of theorems 3.3 and 3.4 in [1], if we recall that $M_{d,1}(n) = \binom{d+n-1}{d} = \binom{d+n-1}{n-1}$. \square

Note that if $W = \mathbf{1}$, the bounds we get are trivial, which means the complexity bounds we will obtain with them will specialize without any difficulty to the known bounds for the homogeneous case.

Using the notation $S = S_n$, we get this new complexity bound for quasi-homogeneous matrix- F_5 :

$$\begin{aligned} C_{F_5} &= O(d_{\text{reg}, M_{d_{\text{reg}}, W}}(n)^\omega) \\ &= O \left(\left(i_{\text{reg}} + \max\{w_i\} \right) \cdot \left[\frac{\delta}{P} \left(i_{\text{reg}} + \max\{w_i\} + S - 1 \right) \right]^\omega \right). \end{aligned} \quad (2)$$

On the other hand, the estimate on the degree of a quasi-homogeneous variety gives the following complexity bound for FGLM: $C_{FGLM} = O \left(n \left(\frac{\tilde{D}}{P} \right)^3 \right)$, where $\tilde{D} = \prod_{i=1}^n d_i$ is the degree of the ideal $\langle \text{hom}_W(F) \rangle$. In the end, for the whole process, we can see that the complexity bounds for our direct strategy is divided by a P^ω factor, when compared to the strategy of going through hom_W .

A consequence of these results is that in general, the higher the weights of the variables, the bigger the gain. In particular, it shows why the applying matrix- F_5 on $\text{hom}_W(F)$ did not yield satisfactory complexity results.

On the other hand, it also shows that when possible, replacing powers of the variables with higher weight variables allows for faster computations of a Gröbner basis. Of course, on a generic homogeneous or quasi-homogeneous system, it won't be possible, but since in practice, the systems we consider are not generic, situations may appear where this idea proves interesting. We will see an example of that in section 4.

3.4 Precise analysis of matrix- F_5

We now fix as goal to follow in a more precise way the computations occurring in the matrix- F_5 algorithm, and to obtain better complexity bounds. For this purpose, we take on the computations made in [2, ch. 3], without proving them whenever the proof is an exact transcription of the homogeneous case.

Let $W = (w_1, \dots, w_n)$ be a weight system, and f_1, \dots, f_m a system of quasi-homogeneous polynomials in $\mathbb{K}[X_1, \dots, X_n]$ which we assume satisfies the hypotheses H1 and H2. We

denote by (d_1, \dots, d_m) the respective W -degrees of the polynomials f_1, \dots, f_m , and we will assume them to allow the existence of such systems.

We also denote by:

- $A_i = \mathbb{K}[X_1, \dots, X_i]$, and $A = A_n$;
- S_i the integer defined in Lemma 9, and $S = S_n$;
- $P_i = \prod_{j=1}^i w_j$, and $P = P_n$;
- $I_i = \langle f_1, \dots, f_i \rangle$, and $I = I_m$;
- $\tilde{I}_i = \langle \tilde{f}_1, \dots, \tilde{f}_i \rangle$, and $\tilde{I} = \tilde{I}_m$;
- $D_i = \deg(I_i) = \prod_{j=1}^i (d_j/w_j)$;
- $\tilde{D}_i = \deg(\tilde{I}_i) = \prod_{j=1}^i d_j$;
- $d_{\text{reg}}^{(i)}$ the degree of regularity of I_i (or of \tilde{I}_i);
- G_i the W -GREVLEX Gröbner basis of I_i as given by matrix- F_5 .

With these notations, we are going to prove the following theorem:

THEOREM 10. Let $W = (w_1, \dots, w_n)$ be a weight system, and f_1, \dots, f_m ($m \leq n$) a system of W -homogeneous polynomials satisfying H1 and H2. Then the complexity of quasi-homogeneous matrix- F_5 algorithm (algorithm 1) is:

$$C_{F_5} = O \left(\sum_{i=2}^m (D_{i-1} - D_{i-2}) M_{d_{\text{reg}}, W}^{(i)}(i) M_{d_{\text{reg}}, W}^{(i)}(n) \right)$$

The goal is to compute precisely how many lines are reduced in a run of the matrix- F_5 algorithm, that is, the number of polynomials in the returned Gröbner basis. This is done by the following proposition, which is a weak variant of [3, th. 10]:

PROPOSITION 11. Let W be a system of weights, and (f_1, \dots, f_m) be a W -homogeneous system satisfying the hypotheses H1 and H2. Let G_i be a reduced Gröbner basis of (f_1, \dots, f_i) for the W -GREVLEX monomial ordering, for $1 \leq i \leq m$. Then the number of polynomials of W -degree d in G_i whose leading term does not belong to $\text{LT}(G_{i-1})$ is bounded by $b_{d,i}$, defined by the generating series

$$B_i(z) = \sum_{d=0}^{\infty} b_{d,i} z^d = z^{d_i} \prod_{k=1}^{i-1} \frac{1 - z^{d_k}}{1 - z^{w_k}}.$$

PROOF. The proof of [3, th. 10] still holds in the quasi-homogeneous case, using formula (1) for the Hilbert series of a quasi-homogeneous regular sequence. \square

So we can obtain a better bound for the number of elementary operations performed in a matrix- F_5 run. Indeed, $B_i(1)$ represents the number of reduced polynomials in the computation of a Gröbner basis of $(f_1, \dots, f_i, X_{i+1}, \dots, X_n)$, that is as many as in the computation of a Gröbner basis of (f_1, \dots, f_i) : since we only perform reductions under the pivot line, [3, prop. 9] shows that the lines coming from X_{i+1}, \dots, X_n will not add any reduction. Note that the above generating series is the same as the Hilbert series of $\langle f_1, \dots, f_{i-1}, X_i, \dots, X_n \rangle$, and so, that its value at $z = 1$ is the degree of that ideal, or D_{i-1} . Therefore, we know that the number of reduced polynomials with label (m, f_i) will be $D_{i-1} - D_{i-2}$ (with convention that $D_0 = 0$).

Now, let g be any polynomial of W -degree d being reduced in a run of the matrix- F_5 algorithm on (f_1, \dots, f_i) . From [3, prop. 9], we know that the leading term of g , after reduction, is in A_i . So overall, in W -degree d , we reduce by at most as many lines as there are monomials in A_i , that is $M_{d,W}(i)$. Furthermore, each reduction costs at most $O(M_{d,W}(n))$ elementary algebraic operations, since this is the length of the

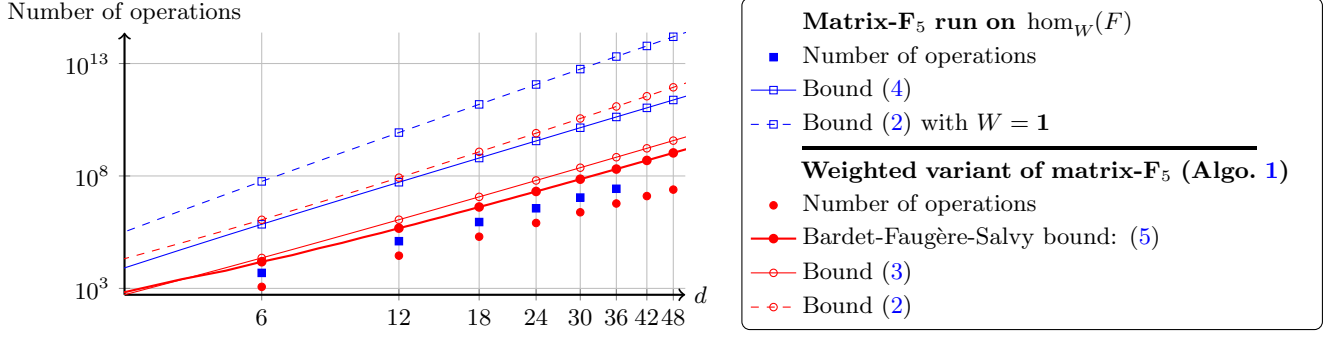


FIGURE 1: Bounds and values, on a log-log scale, for the number of arithmetic operations performed in matrix- F_5 for a generic system with $W = (1, 2, 3)$ and $\mathbf{D} = (d, d, d)$

matrix lines. And we perform these reductions up to degree $d_{\text{reg}}^{(i)}$. Note that, if $i = 1$, there clearly isn't any reduction in the computation, and we obtain the following formulas:

$$\begin{aligned} C_{F_5} &= O\left(\sum_{i=2}^m (D_{i-1} - D_{i-2}) M_{d_{\text{reg}}, W}^{(i)}(i) M_{d_{\text{reg}}, W}^{(i)}(n)\right) \quad (3) \\ &= O\left(\sum_{i=2}^m \frac{1}{P_i P_n} \left(\widetilde{D_{i-1}} - \widetilde{D_{i-2}}\right) \right. \\ &\quad \cdot M_{d_{\text{reg}} + S_i - i + 1, 1}^{(i)}(i) \cdot M_{d_{\text{reg}} + S_n - n + 1, 1}^{(i)}(n) \Big) \end{aligned}$$

In comparison, the above reasoning for matrix- F_5 applied to \tilde{F} would give

$$C_{F_5} = O\left(\sum_{i=2}^m \left(\widetilde{D_{i-1}} - \widetilde{D_{i-2}}\right) M_{d_{\text{reg}}, 1}^{(i)}(i) M_{d_{\text{reg}}, 1}^{(i)}(n)\right) \quad (4)$$

so that here again, working with quasi-homogeneous polynomials yields a gain or roughly P^3 . Note that the exponent 3 (instead of the previous ω) is not really meaningful, because we assumed here that we were using the naive pivot algorithm to perform the Gauss reduction. However, if we assume $\omega = 3$ in the previous computations as well, we observe that our new bound is generally much better than the previous one: figure 1 shows a plot of data obtained both with algorithm 1 and with matrix- F_5 through hom_W , together with the different bounds we can compute.

Asymptotically, though, the gain does not look important, since the complexity is still $O(nD^3)$ where D is the degree of the ideal and $n \geq m$ the number of variables, or in $O(nd^{3n})$ where d is the greatest d_i .

Remark 3. One may also push the computations a bit further, and obtain an even more accurate bound, expressed in terms of the $b_{d,i}$ (these calculations are done in [2] for the homogeneous case, and can easily be transposed to the quasi-homogeneous case):

$$C_{F_5} = O\left(\sum_{i=1}^{m-1} \sum_{d=0}^{\infty} \frac{b_{d+d_{i+1}, i+1}}{P_{i+1} P_n} \cdot M_{d+d_{i+1}+S_{i+1}-i, 1}(i+1) \cdot M_{d+d_{i+1}+S_n-n+1, 1}(n)\right). \quad (5)$$

As an example, we computed that bound as well for a particular case, and included it in figure 1. As can be seen, this bound is indeed better than the intermediate evaluation (3), but the difference is low enough to justify using the latter evaluation. Furthermore, the bound (3) expressed in terms of the D_i 's is more useful in practice, since it has a closed

formula using only the parameters of the system (n, m, d_i and w_i). This allows us to use it in complexity evaluations, in both theory and practice.

Remark 4. As can be seen on figure 1, the number of operations needed by Matrix- F_5 on the homogenized system is not significantly higher than the number of operations needed by the quasi-homogeneous variant of Matrix- F_5 . That is mostly true because the unmodified algorithm can make use of some of the structure of the quasi-homogeneous systems (for example, columns of zeroes in the matrices).

4. THE AFFINE CASE

We will now consider the case of non-necessarily-quasi-homogeneous polynomials. One of the methods to find a GREVLEX Gröbner basis of such a system is to apply F_5 , considering at W -degree d the set of monomials having W -degree lower than or equal to d . This is equivalent to homogenizing the system, that is to adding a variable $X_1 > \dots > X_n > H$ and applying the classical F_5 algorithm to this homogeneous system. The reverse transformation is done by evaluating each polynomial at $H = 1$.

However, this process makes computing the complexity of the F_5 algorithm harder. The main reason is that dehomogenizing does not necessarily preserve W -degree, and as a consequence, it is no longer true that running the matrix- F_5 algorithm up to W -degree d provides us with a basis, truncated at W -degree d . What remains true though is that past some W -degree, we may obtain a Gröbner basis for the entire ideal.

To ease the study, we will only consider *regular in the affine sense* systems (as found in [2]), that is, systems for which no such degree fall may happen.

Definition 2. Let W be a weight system, and (f_1, \dots, f_n) be a system of non-necessarily W -homogeneous polynomials. We write, for any $1 \leq i \leq n$, h_i the quasi-homogeneous component of highest W -degree in f_i . We say that the sequence (f_i) is *regular in the affine sense* when the sequence (h_i) is regular (in the quasi-homogeneous sense). We call *degree of regularity* of the ideal $\langle f_i \rangle$ the degree of regularity of the ideal $\langle h_i \rangle$.

Since a degree fall in a run of matrix- F_5 is precisely a reduction to zero in the highest W -degree quasi-homogeneous components of the system, we know that the F_5 criterion rules out all degree falls in a run of matrix- F_5 on such a regular system.

System	$\deg(I)$	t_{F_5} (qh)	Ratio for F_5	t_{FGLM} (qh)	Ratio for FGLM
Generic $n = 7$, $W = (1, 1, 1, 1, 2, 2, 2)$, $\mathbf{D} = (4, \dots, 4)$	2048	2.7s	1.2	0.43s	2.6
Generic $n = 8$, $W = (1, 1, 1, 1, 2, 2, 2, 2)$, $\mathbf{D} = (4, \dots, 4)$	4096	12.3s	1.8	2.41s	3.0
Generic $n = 9$, $W = (1, 1, 1, 1, 1, 2, 2, 2, 2)$, $\mathbf{D} = (4, \dots, 4)$	16384	314.9s	2.5	119.6s	2.7
Generic $n = 7$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	512	0.09s	3.2	0.06s	1.7
Generic $n = 8$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	1024	0.39s	4.2	0.17s	1.9
Generic $n = 9$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	2048	1.63s	4.9	0.59s	2.0
Generic $n = 10$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	4096	7.54s	5.4	2.36s	2.6
Generic $n = 11$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	8192	33.3s	6.4	17.5s	2.4
Generic $n = 12$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	16384	167.9s	6.8	115.8s	
Generic $n = 13$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	32768	796.7s	8.4	782.74s	
Generic $n = 14$, $W = (2, \dots, 2, 1, 1)$, $\mathbf{D} = (4, \dots, 4)$	65536	5040.1s	∞	5602.27s	
DLP Edwards $n = 4$	512	0.03s	3.7	0.07s	
DLP Edwards $n = 5$	65536	935.39s	6.9	2164.38s	3.2

TABLE 1: Benchmarks with FGb on some affine systems

We can study the complexity of F_5 by looking at a run of matrix- F_5 on the homogenized system. As an example, we prove the following theorem:

THEOREM 12. *Let $W = (w_1, \dots, w_n)$ be a weight system, and f_1, \dots, f_m a generic system of polynomials of the form $f_i = g_i + \lambda_i$, with g_i W -homogeneous of W -degré d_i and $\lambda_i \in \mathbb{K}$. Let D be the degree of the system, d_{reg} its degree of regularity, and δ the gcd of the d_i 's. We can compute a W -GREVLEX Gröbner basis of this system in time*

$$O\left(\frac{d_{\text{reg}}}{\delta^\omega} M_{d,W}(n)^\omega\right),$$

or in other words, we can divide the known complexity of the F_5 process on such a system by δ^ω .

PROOF. The idea is that when we homogenize the system, we can choose any suitable weight for H , not necessarily 1. More precisely, we can set the weight of H to be δ , so that the homogenized polynomials become $f_i^h = g_i + \lambda_i H^{d_i/\delta}$.

This way, assuming the computations made at section 2.2 still hold, we have the same improvements on the bound on d_{reg} and on the size of matrices as before, and we thus have the wanted result.

Note that even if the initial system is generic, the homogenized system is not. However, one can check that if the initial system was regular in the affine sense, the homogenized system is still regular. Indeed, it's enough to check that no reduction to zero occur in a matrix- F_5 run, but it is clear, since such a reduction would in particular be a degree fall. Also, the property of being in Noether position for the m first variables is clearly kept upon homogenizing.

As such, generically, our homogenized system is regular and in Noether position, so the previous computations indeed still hold. \square

5. EXPERIMENTAL RESULTS

We have run some benchmarks¹, using the FGb library [11]. We present these results in Table 1. The examples are chosen with increasing n (number of variables and polynomials), two different classes of systems of weights W and systems of W -degrees D . With these conditions, we built a generic system of polynomials f_i in $\mathbb{F}_{65521}[\mathbf{X}]$, such that all monomials appearing in f_i have W -degree at most d_i . The last examples are systems arising in the study of the Discrete Logarithm Problem, when trying to compute the decompositions of points on an elliptic curve (see [12]).

¹All the systems we used are available online on <http://www-polsys.lip6.fr/~jcf/Software/benchsqhomog.html>.

For each system, we ran the F_5 and FGLM algorithms on both the homogenized system obtained with $\text{hom}_W(t_{F_5}(\text{qh})$ and $t_{FGLM}(\text{qh})$) and the unchanged system (for which we provide the ratio of computing times).

6. REFERENCES

- [1] G. Agnarsson. On the sylvester denumerants for general restricted partitions. *Congressus numerantium*, (154), 2002.
- [2] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, 2004.
- [3] M. Bardet, J.-C. Faugère, and B. Salvy. On the Complexity of the F_5 Gröbner basis Algorithm. (January), 2012.
- [4] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner bases: a computational approach to commutative algebra*. Graduate texts in mathematics. Springer-Verlag, 1993.
- [5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [6] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 10(3):19–29, 1976.
- [7] A. Dickenstein and I. Z. Emiris. Multihomogeneous resultant matrices. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 46–54, 2002.
- [8] D. Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995.
- [9] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, 1999.
- [10] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.
- [11] J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In *Mathematical Software - ICMS 2010*, volume 6327, pages 84–87, 2010.
- [12] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Using symmetries in the index calculus for elliptic curves discrete logarithm. Cryptology ePrint Archive, Report 2012/199, 2012. <http://eprint.iacr.org/>.
- [13] J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.
- [14] J.-C. Faugère and A. Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. In *Advances in Cryptology - CRYPTO 2003*, volume 2729, pages 44–60, 2003.

- [15] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity. *Journal of Symbolic Computation*, 46(4):406–437, 2011.
- [16] R. Hartshorne. *Algebraic geometry*. 1977. Graduate Texts in Mathematics, No. 52.
- [17] J. S. Milne. Algebraic geometry (v5.22), 2012. Available at www.jmilne.org/math/.
- [18] L. Robbiano. On the theory of graded structures. *J. Symb. Comput.*, 2(2):139–170, 1986.
- [19] R. P. Stanley. Hilbert functions of graded algebras. *Advances in Math.*, 28(1):57–83, 1978.